EPSG107-23 v1.0 06/05/2024

Volume v10

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

STANDARDS' REQUIREMENTS

BULLETIN

ON ELLIPTIC-CURVE CRYPTOGRAPHY (ECC) APPLIED TO CARD PAYMENTS

Introduction

The ECSG began addressing the topic of Elliptic-curve cryptography (ECC) in 2021, prior to the publication of the SEPA Cards Standardisation Volume v10 (hereafter, the Volume). At that stage, even though it was recognised as relevant to incorporate ECC into the Volume, the available documentation was not sufficient to define standardisation requirements. It was necessary to wait until 2024 to be able to publish the relevant updates through this bulletin before the publication of the next Volume version.

In the meantime, the association has expanded its scope beyond cards becoming the European Payments Stakeholders Group (EPSG). This bulletin, although published by the EPSG, is related to Volume v10 as published by the ECSG, therefore its ambit is limited to card-based transactions.

This Bulletin includes changes introduced to the following Volume Books:

Book 1 – General principles and definitions:

- New and amended abbreviations, references, and definitions.

Book 2 – Functional requirements:

- Within the table providing an overview of Book 2 Scope, a footnote has been incorporated to clarify that Offline Enciphered PIN encompasses all encryption methods based on RSA or ECC cryptography for the Contact Acceptance Technology as defined in [EMV B2]. Furthermore, XDA and BDHLA have been included as Card Authentication Methods along with the related applicable acceptance technologies.
- Reference to EMV Online Authentication has been adopted within several requirements.
- A modification has been made to a Card requirement for Local Transactions with Chip with Contact, regarding the applicable Card Authentication Methods:
    - for Card Applications supporting ECC-based Offline Data Authentication XDA is mandated;
    - for Card Applications supporting RSA-based Offline Data Authentication the requirement has been simplified.
- A new Card requirement has been introduced for Local Transactions with Chip and Mobile Contactless, mandating BDHLA for ECC-based Offline Data Authentication.
- A modification has been applied to a POI requirement for Local Transactions,
    - specifying for Chip with Contact the applicable Card Authentication Methods:
        - for POI Applications supporting ECC-based Offline Data Authentication XDA is mandated,
        - for POI Applications supporting RSA-based Offline Data Authentication the requirement has been simplified.
    - still indicating that the respective kernel specifications define which Card Authentication Methods are applicable for Chip and Mobile Contactless, but adding that BDHLA is mandated, when Kernel 8 is supported.

- Concerning POI Functional Requirements, a clarification has been introduced regarding Card Authentication for Local Transactions using a Contactless Acceptance Technology, which may include additional kernel-specific mechanisms to detect relay attacks. The respective mechanisms are considered specific to each contactless kernel and beyond the scope of Book 2.

Book 4 – Security requirements:

- Additional list of security features for Local Transactions, covering both Contact and Contactless scenarios.
- Introduction of additional Card Authentication Methods, with ECC-based protocols.
- Amendment to a requirement for Contactless Transactions, referencing EMV® Contactless Specifications for Payment Systems, Book C-2 to C-8, Kernel 2 to 8 Specification, to enhance security against relay attacks.
- Additional requirement for encrypted PIN transmission from the POI to the Card.
- Revised requirement for Contactless Card security during personal data exchange, to ensure protection of sensitive information.
- Amendment to a POI payment application requirement, now including Secure Channel as an integral part of the secure process flow.
- Inclusion of a reference to EMV® Contactless Specifications for Payment Systems, Book E.

While editing this bulletin, a choice was made to incorporate minor editorial improvements, despite their having no direct relevance to ECC. Notably, in Book 4, a clarification regarding the use of signature as cardholder verification method was added, a reference to a now obsolete document was removed in section 3.6.2.1, and specific document version references in section 3.9 were also eliminated. In addition to that, a missing reference to signature use for contactless was added as it reflects the *status quo*. In Book 2, references to EMV specifications have been updated.

Changes introduced into **Book 1 – General principles and definitions**

Changes to section 3. REFERENCES, ABBREVIATIONS AND DEFINITIONS

3.1 References

NB: The last version of a document always applies, except when a specific one is mentioned.

[CPA] EMV Integrated Circuit Card Specifications for Payment Systems, Common Payment Application Specification

[CBP] Regulation (EU) 2019/518 of the European Parliament and of the Council of 19 March 2019 amending Regulation (EC) No 924/2009 as regards certain charges on cross-border payments in the Union and currency conversion charges

[EAA] Directive of the European Parliament and of the Council on the approximation of the laws, regulations and administrative provisions of the Member States as regards the accessibility requirements for products and services (COM/2015/0615 final - 2015/0278 (COD))

[EBA 1] EBA/GL/2014/12 Final guidelines on the security of internet payments

[ECB] ECB/EuroSystem Assessment guide for the security of internet payments

[EMD] Electronic Money Directive - Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision on the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC

[EMV] EMV® Integrated Circuit Card Specifications for Payment Systems, including the Specification Bulletins

[EMV 3DS] EMV® 3-D Secure Specifications

[EMV B1] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements

[EMV B2] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management

[EMV B3] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification

[EMV B4] EMV® Integrated Circuit Card Specifications for Payment Systems, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements

[EMV A] EMV® Contactless Specifications for Payment Systems, ~~(~~Book A, Architecture and General Requirements~~)~~

[EMV B] EMV® Contactless Specifications for Payment Systems, ~~(~~Book B~~)~~, Entry Point Specification

~~[EMV E] EMV® Contactless Specifications for Payment Systems (Book E – Security and Key Management)~~

[EMV C~~1~~2 to C~~7~~8] EMV® Contactless Specifications for Payment Systems~~-~~, ~~(~~Book C-~~1~~ 2 to C-~~7~~8, Kernel 2 to 8 Specification~~)~~

[EMV E] EMV® Contactless Specifications for Payment Systems, Book E, Security and Key Management

[EMV CDCSVM BP] EMV® Consumer Device Cardholder Verification Method— Best Practices, March 2019

[EMV CDCSVM SR] EMV® Consumer Device Cardholder Verification Method Security Requirements

[EMV CMP CM] EMV® Contactless Mobile Payment, Payment Card Management, White Paper

[EMV CMP SE] EMV® Contactless Mobile Payment – PPSE and Application Management for Secure Element

[EMV L1 CL] EMV® Level 1 Specifications for Payment Systems, EMV Contactless Interface Specification

[EMV L1 CT] EMV® Level 1 Specifications for Payment Systems, EMV Contact Interface Specification

[EMV SBMP] EMV® Mobile Payment, Software-based Mobile Payment Security Requirements v 1.1, September 2018

~~[EMV SB185] EMV® Specification Bulletin No. 185, Biometric Terminal Specification~~

[EMVCo-FW v2] EMV® Payment Tokenisation Specification – Technical Framework v2

[EMVCo] EMV Secure Remote Commerce Specifications – API V 1.2

[EMVCo] EMV Specifications – JavaScript SDK V 1.2

[EMVCo] EMV Secure Remote Commerce Specifications – Version Management v 1.0

[EMVCo] EMV Secure Remote Commerce Specifications – Data Dictionary v 1.0

[EMVCo] EMV Secure Remote Commerce Specifications v 1.1

[EMVCo] EMV Secure Remote Commerce User Interface Guidelines and Requirements v1.1.

[EPC Crypto] EPC342-08: Guidelines on algorithms usage and key management

[EPC PS] EPC343-08: EPC Privacy shielding for PIN entry

[EPC Mobile WP] EPC492-09: White paper Mobile Payments

[EPC MCP IIG] EPC178-10: Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines

[FIDO] fidoalliance.org

[FIPS 140-2] Security Requirements for Cryptographic Modules + Annexes

[GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation

[IFR] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions - J.O. May 2015

[ISO/IEC 7810] Identification cards - physical characteristics

[ISO/IEC 7811] Identification cards - Recording technique

ISO/IEC 7811-1: Embossing

ISO/IEC 7811-2: Magnetic stripe - Low coercivity

ISO/IEC 7811-6: Magnetic stripe - High coercivity

ISO/IEC 7811-7: Magnetic stripe - High coercivity, high density

ISO/IEC 7811-8: Magnetic stripe - Coercivity of 51,7 kA/m (650 Oe)

ISO/IEC 7811-9: Tactile identifier mark

[ISO/IEC 7812] Identification cards - Identification of issuers

ISO/IEC 7812-1 Numbering system

ISO/IEC 7812-2 Application and registration procedures

[ISO/IEC 7813] Information technology - Identification cards - Financial Transaction cards

[ISO/IEC 7816-4] Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange

[ISO/IEC 7816-5] Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers

[ISO 8583] Financial transaction card originated messages - interchange message specifications

ISO 8583-1: Messages, data elements, code values

ISO 8583-2: Application and registration procedures for Institution Identification Codes (IIC)

ISO 8583-3: Maintenance procedures for messages, data elements and code values.

[ISO 9564] Financial services - Personal Identification Number (PIN) management and security.

ISO 9564-1: Basic principles and requirements for card-based systems

ISO 9564-2: Approved algorithms for PIN encypherment

ISO/TR 9564-4: Guidelines for PIN handling in open networks

[ISO/IEC 9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher

[ISO/IEC 14443] Information technology - Identification cards -- Contactless integrated circuit cards - Proximity cards

ISO/IEC 14443-1: Physical characteristics

ISO/IEC 14443-2: Radio frequency power and signal interface

ISO/IEC 14443-3: Initialization and anti-collision

ISO/IEC 14443-4: Transmission protocol

[ISO/IEC 15408] Information technology - Security techniques - Evaluation criteria for IT security

ISO/IEC 15408-1: Introduction and general model

ISO/IEC 15408-2: Security functional components

ISO/IEC 15408-3: Security assurance components

[ISO 20022] Financial Services - Universal financial industry message scheme

ISO 20022-1: Metamodel

ISO 20022-2: UML profile

ISO 20022-3: Modelling

ISO 20022-4: XML schema generation

ISO 20022-5: Reverse engineering

ISO 20022-6: Message transport characteristics

ISO 20022-7: Registration

ISO 20022-8: ASN.1 generation

[OMTP1] OMTP Trusted Environment (www.gsma.com)

[OMTP2] OMTP Advanced Trusted Environment (www.gsma.com)

[OMTP3] OMTP Security Threats on Embedded Consumer Devices (www.gsma.com)

[PCI ATM PIN] Payment Card Industry Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Information Supplement: ATM Security Guidelines

[PCI PIN] Payment Card Industry PIN Security Requirements and Testing Procedures

[PCI PTS] Payment Card Industry PIN Transaction Security

[PCI P2PE] Payment Card Industry Point to Point Encryption

[PCI DSS] Payment Card Industry Data Security Standard

[PCI PA-DSS] Payment Card Industry Payment Application Data Security Standard

[PSD] Payment Services Directive - Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

[PSD2] Payment Services Directive 2 - Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015.

[RTS SCA/CSC] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017, supplementing [PSD2] with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

3.2 Abbreviations

Acronym	Standing for	Acronym	Standing for
A2I	Acquirer to Issuer	CB	Certification Board
AAC	Application Authentication Cryptogram	CC	Common Criteria
AAM	Active Account Management	CCD	Common Core Definition
ACS	Access control service	CDA	Combined DDA/Application Cryptogram
AID	Application Identifier	CDCVM	Consumer Device CVM
ATC	Application Transaction Counter	COTS	Commercial Off-The-Shelf
ATICA	Acquirer To Issuer Card Messages	CP	Contactless Payment
ATM	Automated Teller Machine	CPA	Card Payment Application
AVS	Address Verification Service	CPoC	Contactless Payments on COTS
BDH	Blinded Diffie-Hellman	CPS	Card Payment Scheme
BDHLA	Blinded Diffie-Hellman Local Authentication	CSC	Card Security Code
BIN	Bank Identification Number	CVM	Cardholder Verification Method
C2T	Card to Terminal	DCC	Dynamic Currency Conversion
CA	Certification Authority	DCF	Digital Card Facilitator
CAM	Card Authentication Method	DDA	Dynamic Data Authentication
CAPE	Card Payment Exchange	DPA	Digital Payment Application
CAT	Cardholder-Activated Terminal	DTMF	Dual Tone Multi Frequency

ECC	Elliptic Curve Cryptography
ECSG	European Cards Stakeholders Group
EAL	Evaluation Assurance Level
EMV	Europay MasterCard Visa
EPA	Embedded Payment Application
EPC	European Payments Council
EPP	Encrypting PIN Pad
EULA	End User License Agreement
fDDA	Fast Dynamic Data Authentication
GSMA	GSM Association
HMAC	Hash-based MAC
HPP	Hosted Payment Page
HSM	Hardware Security Module
ICC	Integrated Circuit(s) Card
ID&V	Identification and Verification
IF	Interchange Fee
IIN	Issuer Identification Number
IoT	Internet of Things
IFR	Interchange Fee Regulation
ISO	International Organisation for Standardisation
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWS	JSON Web Signature
KBA	Knowledge Based Authentication
KCV	Key Check Value
MAC	Message Authentication Code
MCC	Merchant Category Code
MCP	Mobile Contactless Payment
MIT	Merchant Initiated Transaction
MNO	Mobile Network Operator
MOTO	Mail Order - Telephone Order
MRP	Mobile Remote Payment
NFC	Near-Field Communications
OS	Operating System
OTA	Over The Air
OTP	One Time Password

P2P	Point-to-Point (Encryption)
PAN	Primary Account Number
PAR	Payment Account Reference
PCI	Payment Card Industry
PED	PIN Entry Device
PII	Personally Identifiable Information
POI	Point of Interaction
PPSE	Proximity Payment System Environment
PSD	Payment Services Directive
PSD2	Payment Services Directive 2
PSE	Payment System Environment
PSP	Payment Service Provider
PSU	Payment Service User
PTS	PIN Transaction Security
PVV	PIN verification value
REE	Rich Execution Environment
RP	Remote Payment
REE	Rich Execution Environment
RNG	Random Number Generator
RSA	Rivest–Shamir–Adleman cryptography
SCA	Strong Customer Authentication
SCD	Secure Cryptographic Device
SCRP	Secure Card Reader PIN
SCS	SEPA Cards Standardisation
SDA	Static Data Authentication
SE	Secure Element
SMS	Short Message Service
SPoC	Software-based PIN entry on COTS
SRC	Secure Remote Commerce
SRCI	Secure Remote Commerce Initiator
SRCPI	Secure Remote Commerce Participating Issuer
SRED	Secure Read and Exchange of Data
SSL	Secure Socket Layer
T2A	Terminal to Acquirer
TEE	Trusted Execution Environment
TLS	Transport Layer Security

TOE	Target OF Evaluation (CC)	TSM	Trusted Services Management
TPM	Trusted Platform Module	UI	User Interface
TPP	Third Party Provider	UID	Unique IDentifier
TRSM	Tamper-resistant security module	UPT	Unattended Payment Terminal
TSP	Token Service Provider	XDA	Extended Data Authentication

3.3 Definitions

B.

Blinded Diffie-Hellman (BDH)	The Blinded Diffie-Hellman (BDH) key agreement is a variant of the Elliptic Curve Diffie-Hellman protocol. See [EMV E] for details.
Blinded Diffie-Hellman Local Authentication (BDHLA)	An ECC-based type of dynamic Offline Data Authentication where a dedicated cryptogram (built by the Card Application using transaction data) is authenticated locally by the POI Application using the session key for integrity obtained during a prior Blinded Diffie-Hellman key agreement. See [EMV E], where this method is referred to as "Local Authentication".

C.

Card Authentication	A Function by which the Card Application ~~a chip Card Data~~ is authenticated by the POI Application (Offline ~~Card~~ Data Authentication), by an Additional Authentication Device and/or by the Issuer (EMV Online ~~Card~~ Authentication).

Chip Card (Smart Card)	A carrier into which one or more integrated circuits are inserted to perform processing and memory functions and which supports the contact interface and complies with [EMV L~~B~~1 CT] (referred to as Contact Chip Card) and/or supports the contactless interface and complies with [EMV L1 CL~~D~~] (referred to as Contactless Chip Card). A Chip Card which supports the contact and contactless interface is referred to as Dual Interface Card. A Contact Chip Card as well as a Dual Interface Card complies with [EMV L~~B~~1 CT] and must be of the ID 1 form factor (as defined in ISO/IEC 7810). A Contactless Chip Card which does not support the contact interface may be of the ID 1 form factor (as defined in ISO/IEC 7810), a key fob, or another Form Factor. Note that a Mobile Device is not considered as Chip Card, even if it supports the contactless interface and complies with [EMV L1 CL~~D~~]. The integrated circuits, also referred to as the "chip", carry an EMV Card Payment Application or EMV Card Authentication Application or both, which contains payment card data including but not limited to data equivalent to the Magnetic Stripe data. Also referred to as Smart Card.
Chip Contactless	An Acceptance Technology where Card Data is retrieved from the chip of a Chip Card over the contactless interface compliant with [EMV L1 CL~~D~~]. In this case, the Chip Card is a Contactless Chip Card or a Dual Interface Card and may be of the ID 1 form factor (as defined in ISO/IEC 7810), a key fob, or another Form Factor.
Chip with Contact	An Acceptance Technology where Card Data is retrieved from the chip of a Chip Card over the contact interface compliant with [EMV L~~B~~1 CT]. In this case the Chip Card is a Contact Chip Card or a Dual Interface Card and must be of the ID 1 form factor (as defined in ISO/IEC 7810).

Combined Data Authentication (CDA)	An RSA-based type of ~~offline~~ dynamic Offline ~~d~~Data ~~a~~Authentication where the C~~c~~ard Application combines the generation of a cryptographic value (dynamic signature) ~~for validation by the POI~~ with the generation of an Application Cryptogram, for the POI Application to verify that it originates from a valid card. See [EMV B2].

D.

Dynamic Data Authentication (DDA)	An RSA-based method of dynamic O~~o~~ffline D~~d~~ata A~~a~~uthentication ~~used by a chip enabled device to validate the authenticity of the~~to authenticate ~~chip data and~~ the ~~c~~Card Application by the POI Application, using a P~~p~~ublic K~~k~~ey ~~a~~Algorithm to generate a cryptographic value, including transaction specific data elements.~~, validated by the POI to protect against counterfeit or skimming. Two forms of offline dynamic data authentication are defined by~~ See [EMV B2].~~:~~ ~~DDA and CDA.~~

E.

EMV Online Authentication	Authentication of the Card Application using Application Cryptograms with online communication to the issuer. EMV Online Authentication includes the Card Authentication Methods • ARQC Authentication as specified in [EMV B2] and [EMV B3] as part of "Online Authorisation" (applicable to Chip Contact Acceptance Technology), and • "Remote Authentication" as specified in [EMV E] (applicable to the Contactless Acceptance Technologies).

Extended Data Authentication (XDA)	An ECC-based type of dynamic Offline Data Authentication where the Card Application combines the generation of a cryptographic value (dynamic signature) with the generation of an Application Cryptogram, for the POI Application to verify that it originates from a valid card. See [EMV B2].

F.

Fast Dynamic Data Authentication (fDDA)	An accelerated RSA-based method of Dynamic Data Authentication (DDA) that leverages DDA as defined in [EMV B2 ~~4.3~~] specifications. Used in contactless transactions allowing the POI to issue READ RECORD commands, obtaining DDA related data from the Card Application to perform the DDA calculations after the Card or Mobile Device has left the field.

K.

Kernel	A piece of ~~terminal~~ POI A~~a~~pplication software that contains the interface routines, security and control functions to interact with the Card Application, ~~supports the EMV payment application functions~~ as defined in the EMV specifications. The non-EMV functionality of a POI Application that supports functions like the printer and display, and building messages to send to the acquirer, is not considered part of the kernel.

O.

Offline Biometric Verification	A Cardholder Verification Method defined in [EMV ~~SB185~~], where the biometric data is captured on a Biometric Capture Device and sent to and verified offline by the Physical Card against a biometric reference template stored on the Physical Card

Offline Data Authentication	A process whereby the ~~card~~ Card Application is ~~validated~~ authenticated ~~at the point of transaction~~by the POI Application, using public key technology ~~to protect against counterfeit or skimming~~. ~~Four~~ The following forms of ~~o~~Offline ~~d~~Data ~~a~~Authentication are defined by EMV: • Methods based on RSA: SDA, DDA, CDA and fDDA. • Methods based on ECC: XDA and BDHLA.
Offline Enciphered PIN	An Offline PIN whereby the PIN is transmitted to the card encrypted using an RSA- or ECC-based P~~p~~ublic ~~k~~Key ~~cryptography~~ Algorithm at the POI's PIN Entry Device. See [EMV B2].

S.

Secure Channel	A security mechanism described in [EMV E] to provide confidentiality between the POI Application and the Card Application for contactless transactions.

Static Data Authentication (SDA)	An RSA-based type of O~~o~~ffline ~~Card ~~D~~d~~ata A~~a~~uthentication where the POI validates a cryptographic value stored on the card by the issuer (as defined in [EMV B2]). It protects against some types of counterfeit fraud but does not protect against skimming.

Changes introduced into **Book 2 – Functional Requirements**

Changes to section 2. SCOPE

[…]

Table 4 below represents the scope of Book 2 and lists for Local and Remote Transactions which of the following items are or are not covered by the Volume (this is indicated by a "Y" or "N" respectively):

⇒ Card Services

⇒ Cardholder Environments and Acceptance Environments

⇒ Acceptance Technologies

⇒ Cardholder Verification Methods and Card Authentication Methods

"Y" also indicates that the item is allowed for a specific type of transaction.

"N" also indicates that the item is not allowed for a specific type of transaction.

"N/A" indicates that the item is not covered in this version of the Volume but may be covered in future releases.

Definitions of the different Card Services, Cardholder Environments, Acceptance Environments, Acceptance Technologies, Cardholder Verification Methods, Card Authentication Methods and Functions are provided in Book 1.

	SCS Volume Book 2 Scope	
	Transactions	
	Local	Remote
CARD SERVICES		
PAYMENT SERVICES		
Payment	Y	Y
Refund (partial or total)	Y	Y
Cancellation	Y	Y

	SCS Volume Book 2 Scope	
	Transactions	
	Local	Remote
Pre-Authorisation Services • Pre-Authorisation • Update Pre-Authorisation • Payment Completion	Y	Y
Deferred Payment	Y	N
No-Show	Y	Y
Instalment Payment	Y	Y
Recurring Payment	Y	Y
Quasi-Cash Payment	Y	Y
CASH SERVICES		
ATM Cash Withdrawal	Y	N
Cash Advance (Attended)	Y	N
Cash Deposit	N/A	N/A
CARD ENQUIRY SERVICES		
Card Validity Check	Y	Y
Balance Enquiry	Y	N/A
CARD ELECTRONIC TRANSFER		
Card Fund Transfer	Y	Y
Original Credit	Y	Y
Prepaid Card – Loading & Unloading	Y	Y
e-Purse - Loading/Unloading	N/A	N/A
ADDITIONAL FEATURES		
Payment with Increased Amount	Y	N
Payment with Cashback	Y	N
Payment with Purchasing or Corporate Card Data	Y	Y
Payment with Aggregated Amount	Y	Y
Payment with Deferred Authorisation	Y	Y
Dynamic Currency Conversion (DCC)	Y	Y
Surcharging/Rebate	Y	Y
Payment with Deferred Clearing	N/A	N/A

	SCS Volume Book 2 Scope	
	Transactions	
	Local	Remote
Payment with Loyalty Information	N/A	N/A
Unsolicited Available Funds	N/A	N/A
CARD MANAGEMENT SERVICES		
PIN Change / Unlock	N/A	N/A
Card Activation	N/A	N/A
Return Card to Cardholder Request	N/A	N/A
Card Pick-up Advice	N/A	N/A
Return Card Advice	N/A	N/A
ACCEPTANCE TECHNOLOGIES		
Chip with Contact	Y	N
Magnetic Stripe	Y	N
Chip Contactless[8]	Y	N
Mobile Contactless[8]	Y	N
Manual Entry by Acceptor[9]	Y	Y[10]
Manual Entry by Cardholder	N	Y[11]
Stored Card Data (stored by the Acceptor)	Y	Y
Consumer Device with Payment Credentials	N	Y
Consumer Device with Payment Credentials and Authentication Application	N	Y
Consumer Device with (M)RP Application	N	Y
Imprint	N/A	N/A

[8] If it is not necessary to distinguish the Cardholder Environment in use, Chip Contactless and Mobile Contactless are referred to as Contactless Acceptance Technology, because they are both implementations of [EMV L1 CL] and communication and behaviour are the same from the perspective of the POI.

[9] Acceptor may also stand for an Attendant in the Acceptor's environment.

[10] Not applicable to e- and m-commerce.

[11] For MOTO only if a touch-tone facility on a telephone handset is supported for Telephone Orders.

	SCS Volume Book 2 Scope	
	Transactions	
	Local	Remote
CARDHOLDER ENVIRONMENTS		
Physical Card	Y	Y
Consumer Device	Y[12]	Y
Virtual Card	N	Y
ACCEPTANCE ENVIRONMENTS		
Physical POI		
Attended[13]	Y	Y[14]
Unattended	Y	N
Remote POI		
Virtual POI	N	Y[15]
Virtual Terminal	N	Y[14]
CARDHOLDER VERIFICATION METHODS		
Offline Plaintext PIN[16]	Y	Y
Offline Enciphered PIN[16, 17]	Y	Y
Online PIN	Y	N
Signature	Y	N[18]
No CVM Required	Y	Y[19]
Offline Biometric Verification	Y	Y
Biometrics via Sensor on Card	Y	Y

[12] Using the Mobile Device for Mobile Contactless.

[13] According to the definition in Book 1, this Acceptance Technology also comprises Semi-Attended.

[14] Not applicable to e- and m-commerce.

[15] Not applicable to MOTO.

[16] Where this Book refers to "Offline PIN", it is referring to both Offline Plaintext PIN and Offline Enciphered PIN.

[17] Offline Enciphered PIN encompasses all encryption methods based on RSA or ECC cryptography for the Contact Acceptance Technology as defined in [EMV B2].

[18] However, a mail order form contains a cardholder signature.

[19] The No CVM Required covers the verification process defined by EMV and other cases where Cardholder Verification is not required (see 4.2.3.7.2).

	SCS Volume Book 2 Scope	
	Transactions	
	Local	Remote
Biometrics on Consumer Device (CDCVM)[20]	**Y**	**Y**
Offline Mobile Code (CDCVM)[20]	**Y**	**Y**
Online Mobile Code	**N**	**Y**
Offline Personal Code (CDCVM)[20]	**N**	**Y**
Online Personal Code	**N**	**Y**
CARD AUTHENTICATION METHODS		
SDA	**Y**	**Y**
DDA	**Y**	**Y**
CDA	**Y**	**Y**
fDDA[21]	**Y**	**N**
XDA	**Y**[22]	**N**
BDHLA	**Y**[21]	**N**
EMV Online Authentication	**Y**	**Y**
Static Authentication[23]	**Y**	**Y**
Dynamic Authentication - One Time Password (OTP)[24]	**N**	**Y**
Dynamic Authentication - Challenge Response based on Additional Authentication Device[25]	**N**	**Y**
Dynamic Authentication - Challenge Response based on Authentication/Remote Payment Application on a Consumer Device[25]	**N**	**Y**
FUNCTIONS		
Configuration	**Y**	**Y**
Transaction Initialisation	**Y**	**Y**

[20] Biometrics on Consumer Device, Offline Mobile Code and Offline Personal Code are the types of CDCVM defined in the Volume.

[21] Only applicable to the ~~c~~Contactless Acceptance Technologies.

[22] Only applicable to the Contact Acceptance Technology.

[23] Typically the Card Security Code (CSC) is used.

[24] This Card Authentication Method is used for e- and m-commerce and may use EMV authentication methods.

[25] This Card Authentication Method is used for e- and m-commerce and may use EMV or FIDO authentication methods.

	SCS Volume Book 2 Scope	
	Transactions	
	Local	Remote
Language Selection	Y	Y
Technology Selection	Y	N
Selection of the Application	Y	Y
Card Data Retrieval	Y	Y
Card Authentication	Y	Y[26]
Cardholder Verification	Y	Y
Authorisation	Y	Y
Referral	Y	N
Completion	Y	Y
Reversal	Y	Y
Data Capture	Y	Y
Financial Presentment	N/A	N/A
Settlement	N/A	N/A
Chargeback	N/A	N/A
ADMINISTRATIVE SERVICE		
Reconciliation	N/A	N/A

Table 4: Book 2 Scope

[…]

[26] Cardholder authentication is an important issue in the remote environment. In this environment the boundaries between authentication and / or verification of the Card and the Cardholder may become blurred. However, for this version of the Volume, the functions Card Authentication and Cardholder Verification have been kept separate to respect compatibility with the functions defined for Local Transactions.

Changes to section 3. FUNCTIONAL REQUIREMENTS FOR CARDHOLDER ENVIRONMENTS

[…]

3.3.1 Chip with Contact

Req C1: The Physical Card-to-Reader communication shall be compliant with [EMV L~~B~~1 CT]. The functionality (commands and data structure) implemented by Card Applications shall comply with the relevant requirements in [EMV B1].

Req C2: Physical Cards shall support Application Selection through PSE according to [EMV B1][30].

Req C3: PSE and Card Applications shall include the Language Preference data element and the Application Selection Registered Proprietary Data.

It is recommended that the Language Preference also includes English to ease use in international markets.

The Application Selection Registered Proprietary Data with ID = '0001' shall be present:

- In the Directory Discretionary data (tag '73') within every ADF Directory Entry,
- AND in the FCI Issuer Directory Discretionary data (tag 'BF0C') within the FCI of every ADF.

Req C4: Card Applications shall support Offline and Online PIN as CVM. Other CVMs as defined by [EMV] ~~or [EMV SB185]~~ may also be supported.

Card Applications may support either Offline Enciphered PIN or Offline Plaintext PIN or both. Offline Enciphered PIN is preferred and required for newly issued and replacement cards. Offline Plaintext PIN may still be present in the CVM List for use outside EEA, but only with a lower priority than Offline Enciphered PIN.

The requirement to support PIN may be waived in exceptional circumstances, to allow Card Transactions by people who, for reasons of disability, are unable to enter, memorise and/or safeguard a PIN.

[30] The support of "Payment System Environment" (PSE) by the Physical Card is optional in [EMV B1]. The support of PSE is mandatory for SEPA compliance as defined in Req C2.

Req C5: Card Applications shall support EMV Online Authentication~~ as defined by [EMV]~~.

Req C6: The following applies for Card Applications that support ~~offline transactions~~RSA-based Offline Data Authentication~~ shall support Offline Data Authentication as follows~~:

- ~~SDA is not permitted on newly issued cards.~~
- DDA is ~~mandatory~~optional.
- CDA is mandatory~~ on newly issued cards~~.
- SDA is not permitted~~ on newly issued cards.~~
-

For Card Applications that support ECC-based Offline Data Authentication, XDA is mandatory.

3.3.2 Chip and Mobile Contactless

For Mobile Contactless Card Applications and Mobile Devices additional guidance can be found in [EPC MCP IIG].

Req C7: The Physical Card or Mobile Device-to-Reader communication shall be compliant with [EMV L1 CL].

Req C8: (Mobile) Contactless Card Applications shall comply with any card requirements in [EMV A] and [EMV B].

Req C9: The (Mobile) Contactless Card Application shall allow identification of the Form Factor for use in authorisation and data capture.

Req C10: Physical Cards and Mobile Devices shall support Combination Selection through PPSE according to the card requirements in [EMV B].

Req C11: For the management of multiple Mobile Contactless Card Applications, Mobile Devices shall be compliant with [EMV CMP CM] and, if applicable, with [EMV CMP SE].

Req C12: The PPSE and the Card Applications shall include the Application Selection Registered Proprietary Data.

The Application Selection Registered Proprietary Data with ID = '0001' shall be present:

- In every Directory Entry (tag '61') within the FCI of the PPSE,
- AND in the FCI Issuer Directory Discretionary data (tag 'BF0C') within the FCI of every ADF.

Req C13: Physical Cards that support Biometrics via Sensor on Card shall indicate this CVM to the POI as CDCVM.

Req C14: A Mobile Contactless Card Application that supports Online Mobile Code shall indicate this CVM to the POI as CDCVM.

Req C21: For Contactless Card Applications that support ECC-based Offline Data Authentication, BDHLA is mandatory.

Changes to section 4. POI FUNCTIONAL REQUIREMENTS

[…]

4.2.3.6 Card Authentication

4.2.3.6.1 Local Transactions (Physical POI)

Card Authentication for Local Transactions is the Function defined by EMV by which a Card Application is authenticated to the POI (Offline Data Authentication) and/or the Issuer (EMV Online Authentication). Card Authentication applies only to the Chip with Contact Acceptance Technology and to the Contactless Acceptance Technology.

Card Authentication for Local Transactions using a Contactless Acceptance Technology may contain additional steps to detect relay attacks. These mechanisms are specific to each contactless kernel[34] and are out of scope of this document.

Req T64: Online-only POI Applications are not required to support Offline Data Authentication.

Req T65: The following applies for POI Applications supporting the Chip with Contact Acceptance Technology and RSA-based Offline Data Authentication~~ shall support the Offline Data Authentication methods as defined in [EMV] as follows~~:

- ~~SDA is optional.~~
- DDA is mandatory.
- CDA is mandatory~~ for newly installed POI~~.
- SDA is ~~optional~~no longer supported.

For POI Applications supporting the Chip with Contact Acceptance Technology and ECC-based Offline Data Authentication, XDA is mandatory.

For ~~the~~ POI Applications supporting ~~the~~ Chip and Mobile Contactless~~ Acceptance Technology~~, the Offline Data Authentication methods shall be supported as defined in the respective kernel specifications (in particular BDHLA, when supporting Kernel 8 [EMV C8]).

[34] E.g. Relay Resistance Protocol in [EMV C8].

[…]

4.2.3.7 Cardholder Verification

[…]

4.2.3.7.1.2 Cardholder Verification for the Chip with Contact Acceptance Technology

Req T72: POIs with a PIN Entry Device shall meet the following requirements:

- For POIs which are not ATMs:
  - For offline-only POIs the POI Application shall support Offline PIN.
  - For offline with online capability POIs the POI Application shall support Offline PIN and may support, in addition, Online PIN.
  - For online-only POIs the POI Application shall support Offline PIN, or Online PIN or both.
  - Other CVMs as defined by [EMV]~~ or [EMV SB185]~~, including Signature, No CVM Required and Offline Biometric Verification, may be supported in addition to PIN.
  - Unattended POIs shall not support Signature CVM and Combined CVM containing Signature.
- For ATMs:
  - The POI Application shall support Online PIN.
  - The POI Application may in addition support Offline PIN and Offline Biometric Verification.
  - ATMs shall not support No CVM Required, Signature CVM or Combined CVM containing Signature.

Changes introduced into **Book 4 – Security Requirements**

Changes to section 2. DESCRIPTION OF SECURITY FEATURES FOR CARD TRANSACTIONS

[…]

2.2. Local Transactions – Contact and Contactless

For local transactions, a number of well-established security features are implemented in the market and used by the stakeholders. This includes

- Card Authentication
- Cardholder Verification
- Data protection using a secure channel
- Security measures against relay attacks.

In the context of this book, a distinction is made between whether a physical card (contact or contactless) or a mobile contactless payment application accessed via a mobile device is involved. The security features for both are specified in the relevant sections of the EMV books (see [EMV]).

2.2.1. Card Authentication, Data Protection and Cardholder Verification Methods

This document provides a high level overview of the different Card Authentication and Cardholder Verification Methods (CVMs) for local transactions.

The mobile environment offers a number of additional features which can be utilised for mobile contactless card payments with respect to CVMs compared to contactless card payments using physical cards. For mobile contactless, the EPC Mobile Contactless SEPA Card Interoperability Implementation Guidelines [EPC MCP IIG] may also be consulted for further guidance.

	Contact	Contactless
Card Authentication		
DDA*	X	

fDDA**		X	
CDA*	X	X	
XDA*	X		
BDHLA****		X	
Data Protection			
BDH****		X	
CVMs	**Card**	**Card**	**Mobile**
Physical POI CVM			
Online PIN	X	X	X
Offline PIN	X	X	
Offline Biometrics	X	(see definition in Book1)	
Signature*****	X	X	
No CVM Required	X	X	X
Cardholder Device CVM (CDCVM)			
Biometrics			X

Mobile code***			X
Other Methods			
Biometrics via Sensor on Card	(see definition in Book1)	X	

FIGURE 1: OVERVIEW OF CARD AUTHENTICATION AND CARDHOLDER VERIFICATION METHOD

*See [EMV B2] sections 6 and 12~~.x and 6.6~~

**See [EMV C3]

*** Mobile code[1]: entered on the mobile device.

- The verification of the mobile code is done by the MCP application in the SE on the mobile device;

or

- Implicit validation of the correct entry of the mobile code through a cryptographic derivation, verified on-line by the MCP issuer, typically used for HCE-Based systems (see 2.2.3.2).

**** See [EMV E]

*****Although Signature is not recognised as a valid authentication factor in the context of SCA, it is listed here for implementations that rely on Signature with Chip Cards.

One approach to a “mobile payment using a Consumer Device User/Cardholder Verification Method” (refer to as CDCVM Solution) is described in [1].

[1] For security reasons, in case of a mobile code, this is a dedicated mobile code (also referred to as mobile PIN, mobile passcode, etc.) which differs from the "classic" card PIN.

A **CDCVM Solution** may be provided at application level (Card / Authentication Application), and/or at device or OS level as a mobile platform authentication mechanism for use by mobile applications on the device ("shared CDCVM").

It has to be ensured that the CDCVM Solution cannot be maliciously abused, disabled or bypassed; and that its assets are adequately protected. The key security goals and objectives for the steps involved in CDCVM processing (e.g. biometry, mobile code) are:

- **Capture**: Secure processing of the (raw) entry data, secure channel for transfer of CVM data
- **Feature extraction**: Secure extraction / conversion of input into a format suitable for matching with a reference; secure channel for transfer of sample (if applicable).
- **Match**: Secure channel for transfer of stored reference data, secure matching process; and secure channel for transfer of the result of the matching process through the Authenticator APIs

A number of **CDCVM Assets** must be protected, depending on the CDCVM solution. Assets can be categorized as requiring one or more security services: Confidentiality (e.g. Biometric Image), Integrity (e.g. Verification Result), and Integrity with the addition of accountability/authentication (e.g. Biometric Processing Firmware).

[…]

Changes to section 3. SECURITY REQUIREMENTS

[…]

3.4. Security Requirements for Card Services

3.4.1. Local transactions

[…]

3.4.1.2. Chip and Mobile Contactless

For Contactless Transactions, the relevant Security Requirements defined by EMV in [EMV E] shall apply. In addition, the following requirements shall apply:

Req S5: For Card Authentication for contactless transactions, dynamic authentication as described in section 2.2 shall be performed.

Req S6: The risk parameters "Acquirer CVM Limit", "Floor Limit" and "Transaction Limit" shall be supported by the Physical POI.

Req S7: The acquiring systems and protocols used shall be able to support the authentication methods and the CVM methods, as appropriate, described in section 2.2.1.

Req S8: If a PIN/CDCVM is used for CVM, then they shall be used in conjunction with a PIN/CDCVM Try Limit and with a PIN/CDCVM Try Counter[4].

Req S9: Mechanisms ~~shall~~ may be made available by the Card and the POI to safeguard against relay attacks as defined by EMV in~~[EMV BE] and~~ [EMV C8].

[4] Where there are a number of applications on a single device using the same CVM reference data, there should be a common Try Counter.

3.5. Cardholder Verification

This section provides security requirements for the following CVMs: PIN, Personal and CDCVM.

3.5.1. PIN Security Requirements

When the PIN is entered and processed, it shall be protected using the appropriate security standards as defined in PCI PIN Security Requirements and the other standards referenced therein.

ISO 9564 is the established baseline for protecting PINs during online transmission. The PIN should be protected by an ISO PIN block format.

Req S24: For online transactions, PINs shall be formatted according to ISO 9564-1 PIN block formats 0, 1, 3 or 4 prior to encryption and shall be encrypted using a dynamic encryption method like DUKPT (Derived Unique Key Per Transaction) or UKPT (Unique Key Per Transaction). Format 1 should be avoided when the PAN is available.

Req S25: Format 2 shall only be used for PINs that are submitted from the ICC reader or the PED, to the ICC chip. If the PIN-block is sent encrypted to the ICC it shall be formatted in an encryption block according to ISO 9564, prior to encryption.

Req S26: PIN translation from one ISO PIN block format into another shall follow the PIN block format translation restrictions defined in ISO 9564-1.

Req S27: If random values are not used for key derivation, unique key methods shall be applied. Such methods may involve the use of uni-directional, dynamic session keys (i.e. shall not involve the use of fixed transaction keys). This applies to POI-to-Host and is recommended for Host-to-Host communication.

PIN encryption from the POI to the Issuer is a mandatory requirement for all online-to-issuer PIN transactions, in particular:

Req S28: The PIN shall be encrypted inside a TRSM (PIN pad or PED) where the PIN is entered by the cardholder at the POI.

Req S29: The PIN shall be translated from one cryptographic zone to another, inside an approved hardware security module (HSM) at a non-issuer host system, e.g. acceptor and acquiring host.

For PIN transmission from the POI to the Card the following requirement applies:

Req S43: The PIN shall always be transmitted encrypted.

3.6. Security Requirements for Card Environments

3.6.1. Security Requirements for Physical Chip Cards

[…]

3.6.1.4. Contactless Card Security Requirements

For Contactless Cards the Security Objectives from paragraph 3.6.1.4 apply. In addition, the following Security Objectives are defined for Contactless Cards.

CC	Contactless Cards	
CC1	O.DI_CONTACTLESS_COUNTERS	When required by applicative specifications, DI (Dual Interface) cards shall manage internal counters such as counters limiting their use in contactless mode without PIN verification (e.g. unitary and cumulated amounts). DI cards shall protect them to the same level as they do for sensitive counters such as transaction counter (ATC) or PIN try counter (PTC). The integrity and their capability shall not allow them to be bypassed.
CC2	O.DI_PRIVACY	Relevant personal data present on the card (e.g. Cardholder Name, Log File) shall ~~not~~ only be exchanged encrypted using a session key established for a Secure Channel through contactless transactions. If such a Secure Channel cannot be established, these relevant personal data shall not be exchanged through contactless transactions.
CC3	O.DI_DOS	DI cards shall not be blocked, e.g. when receiving a series of wrong APDU-Commands and shall still continue to answer with an Error code in the APDU response.

TABLE 9: CONTACTLESS CARDS SECURITY REQUIREMENTS

[…]

3.6.2. Security requirements for Mobile Contactless Payment Applications residing in a Secure Element

[…]

3.6.2.1. Scope of the Evaluation

The Target of Evaluation includes all hardware and software parts of the SE and MCP application needed to perform the payment functionality and to enforce its security.

SE and MCP application functionality, can consist of transactions and possibly also card management functions, as specified by each payment scheme. In this respect, it is assumed that the following basic capabilities are supported:

- Application Selection (at SE level);
- Initiate Application Processing;
- Off-line communication with the POI;
- Off-line Data Authentication~~ (as described in *[EPC1]*)~~;
- On-line authentication and communication with the issuer~~ (as described in *[EPC1]*)~~;
- CVM (see section 2.3.2.2);
- MCP risk management;
- Transaction Certification;
- Script processing (to update MCP application parameters and software);
- Internal State Management, ensuring that the above functions are performed in a coherent way.

[…]

3.7. POI Security Requirements

3.7.1. Physical POI (for local transactions)

[…]

3.7.1.2. Life Cycle

[…]

Section G- Requirements for the POI payment application **Note: All section G are ECSG+ requirements**	
G1 **ECSG+**	The POI provides security functions. These security functions *shall* be called by the payment application according to a secure process flow as defined by the payment application. The following security functions *shall* be considered as part of the secure process flow. a) Establishing and using the Secure Channel, if supported by both POI, and Card ~~PIN entry~~ b) Confirmation of the amount c) PIN entry ~~Verification of the online and offline result~~ d) Prompting of the transaction result e) Verification of the online and offline result ~~Maintaining security related transaction data~~ ~~e)~~f) Maintaining security related transaction data ~~Establish and maintaining the Secure Channel, if supported by both POI, and ard~~ Note: This ECSG+ requirement is covered within the PCI PTS standard by multiple requirements including requirements A4, A7, B2, B14 and B15. This ECSG+ is retained for ease of adoption by other schemes.

3.7.1.3. *Applicability of Requirements*

[…]

Requirements for the POI payment application (optional except G1 ECSG+)													
G1 ECSG +												x	Depends upon AB/CPS
G1.1 ECSG +												x	Depends upon AB/CPS
G1.2 ECSG +												x	Depends upon AB/CPS
G1.3 ECSG +												x	Depends upon AB/CPS
G2 ECSG +												x	Depends upon AB/CPS
G3 ECSG +												x	Depends upon AB/CPS
G4 ECSG +												x	Depends upon AB/CPS
G5 ECSG +												x	Depends upon AB/CPS

Table 22: Supported Functionalities

[…]

3.9. Security Requirements for Automated Teller Machines ATMs

This section defines the minimum applicable security requirements for ATMs.

Req S36: The requirements defined in section 3.7.1.1 using the “PIN Entry” functionality of the Applicability Matrix provided in section 3.7.1.2. apply.

Req S37: The ATM shall support the authenticity of the EPP by cryptographic means. For authentication purposes the EPP shall have a unique identifier which shall be implemented by a secure initialisation process. This identifier shall not be modified or outputted without notice.

Approval to use a certified product in a particular market remains with the relevant Approval Body or Card Payment Scheme, the process for which is detailed in Book 5.

Guidance for more detailed security requirements are given in

- [EMV B2] EMV, Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management~~, Version 4.1, Mai 2004~~,
- [EMV E] EMV, Contactless Specifications for Payment Systems, Book E~~, Version 1.0, xxx 2023~~
- [PCI ATM PIN] Transaction Security Point of Interaction Security Requirements (PCI PTS POI), ~~Version: 1.0, Date: January 2013,~~ Information Supplement: ATM Security Guidelines